

AD-A049 110

RAND CORP SANTA MONICA CALIF
RPVS, DATA LINKS, AND THE JAMMING THREAT, (U)
MAY 77 J W ELLIS
RAND/P-5865

F/G 17/4

UNCLASSIFIED

NL

| OF |
ADAO49110



END
DATE
FILMED
2 - 78
DDC

AD A049110

AD No.
FILE COPY

2 B.S.

6

RPVS, DATA LINKS, AND THE JAMMING THREAT,

10

John W. Ellis, Jr.

11

May 1977

12

33 p.

14

RAND/P-5865

DDC
RECEIVED
JAN 30 1978
AF

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

P-5865

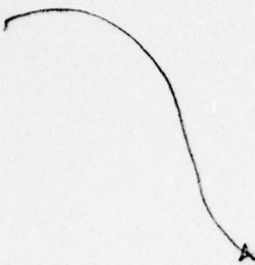
296600 B

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional Staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.


The Rand Corporation
Santa Monica, California 90406

ABSTRACT



Soviet exploitation of their own technological developments has produced increasingly strong forward battle area surface-to-air defenses and, at the same time, strengthened the need for our own combat fire support to help offset the massive enemy ground force fire power advantage. Recent technological innovations on our part--e.g., standoff munitions, homing weapons, remotely piloted vehicles--promise to alleviate this situation, but the data links needed by many of these new devices present a new, and potentially attractive, vulnerability that the enemy defense may be able to exploit.

Analysis of that potential vulnerability requires a contextual systems approach rather than the traditional one-on-one. This means including system life-cycle costs, examining alternatives open to both sides other than simply entering into an electronic countermeasures/counter-countermeasures game, and assessing the utility of those alternatives in terms of a total combat system payoff criterion. Within this context, an approach is discussed that can help identify those circumstances favoring the enemy use of jammers and the resultant data link jam-resistance performance requirements and allowable costs.



This paper was presented at the 1977 Air University Airpower Symposium, "The Impact of Technology on Air Warfare," Air War College, Maxwell Air Force Base, Alabama, on 30 March 1977.

ENCLOSURE PAGE NOT FILLED
BLANK

ACKNOWLEDGEMENTS

The author wishes to express his appreciation to his Rand colleagues, D. E. Lewis, T. M. Rodriguez, and J. Schank, for many helpful discussions. In particular, he is indebted to J. R. Hiland and J. Lau for their contributions to the development and clarification of the issues discussed in Sections VII through XI.

ACCESSION for	
NTIS	Write Section <input checked="" type="checkbox"/>
DDC	B ff Section <input type="checkbox"/>
UNANNOUNCED	<input type="checkbox"/>
J S I CATION	
<i>on file</i>	
BY	
DISTRIBUTION/AVAILABILITY CODES	
SPECIAL	
<i>A</i>	

RPVS, DATA LINKS, AND THE JAMMING THREAT

The introduction of the products of advancing technology is causing important changes in the classical tactical battlefield environment that, since World War II, has been the accepted image of conventional combat. Microelectronics have made possible (at relatively low cost) small, light-weight computers, high-resolution optical and IR imaging sensors, a variety of accurate homing devices, wide-band links, etc. that can provide the combat soldier and airman with capabilities never before available to him.¹ Since technology knows no national allegiance and its exploitation by one side quite often opens technological opportunities for the other to employ countermeasures, we must always be alert to any potential vulnerabilities introduced in our own attempts to utilize new developments. At the same time, one must not let his imagination unreasonably magnify such potential vulnerabilities that can attend the introduction of new technologies to the point of inhibiting progress. A current example of this dilemma revolves around the vulnerability to jamming of the RPV data link. Much of the reluctance to press for early incorporation of RPVs into operational use is due to the widely-held belief that data links are easy and cheap for the enemy to jam and, conversely, difficult and expensive for the U.S. to provide adequate jam resistance. The remainder of this

¹A useful overview of the potential applicability and utility of devices made possible by technological developments is contained in Ref. 1.

paper will explore a new approach to the analysis of this problem. But, first we must define the context within which the present discussion will be carried out and indicate what motives there are for concerning ourselves with an RPV, much less with the vulnerability of its data link to electronic countermeasures.

II

Beginning with the renewed interest in RPVs early in this decade, their application to many military functions has been proposed and explored by each of the Services and their contractors.² Notwithstanding the promise of some of these other proposed uses, for the present purpose, RPVs, data links, and the electronic countermeasures game will be addressed only in the context of conventional tactical conflict and, in particular, will deal only with the interplay of forces and instrumentalities in the forward battle area. In exploiting its own developing technologies, the Soviet Union has chosen to design and deploy large numbers of radar-guided surface-to-air missiles, man-portable IR homing missiles, and relatively small calibre, high rate of fire anti-aircraft guns. The latter, if not due to a startling technological breakthrough, are the result of engineering improvements in a technology many had considered deserving of little further interest in the era of ground-to-

²A summary of possible applications for RPVs that derived from an AFSC/Rand Corporation symposium (held in July 1970) is contained in Ref. 2. An extensive review of Service programs is in Refs. 3-6.

air missile defenses. Consequently, as presaged by the operational evidence from Southeast Asia and the Middle East, on future tactical battlefields, friendly air forces will face a technologically advanced and highly dense air defense system whose overlapping effectiveness extends from the nap of the earth to essentially the top of the atmosphere. Moreover, in recent years, Soviet surface-to-air defense trends have been toward greater mobility. This trend, in itself, has several important facets. A greater proportion of the defensive elements have been made mobile, and their degree of mobility has been enhanced. This has encouraged, through smaller unit size and lower unit cost, proliferation of forces and eased their concealment. Hence, battlefield defenses have become harder to avoid or detect and attack.

At the same time, the Soviet Field Armies in Europe developed highly mobile forces containing large numbers of relatively hard combat elements (e.g., tanks, APC, and artillery) supported by highly redundant, hardened command and control centers, aircraft shelters, etc. Facing this threat the defending NATO ground forces are at a severe fire power disadvantage.³ Increasing the volume and rate of fire in support of friendly units and extending the range and depth over which fire can be concentrated can help redress the imbalance.

³One of the more recent analyses of the relationship between NATO and Warsaw Pact forces is contained in Ref. 7. See particularly pp. 13-15 on the inadequacy of current NATO fire power levels.

Contextual and technological developments (on both sides) are forcing a reevaluation of the classical ground/air battlefield environment. The enemy tactical air defense system, unless countered, will seriously decrease the capability of air forces to provide the required fire support to friendly ground forces. Presumably, the latter condition is a goal indicative of the enemy's concern for the effect of that fire power on his own forces. Three possible responses to permit delivery of fire support in the face of highly effective, mobile, and proliferated air defenses are: employ stand-off weapons to alleviate the need for penetration in providing aerial fire support; reduce the air defense effectiveness to a tolerable level by using various penetration aids (decoys, jamming, harassment, etc.); or destroy the defenses. To successfully deliver weapons against ground targets (by whatever means--manned aircraft, RPVs, or standoff missiles), it is necessary to accomplish a variety of prerequisite and supporting functions such as reconnaissance, surveillance, target development, identification, and acquisition, laser designation for guided weapons, fire adjustment, and strike control.

III

This diverse set of missions can be satisfied by a relatively small number of functional capabilities: observation of the area or item of interest with an appropriate sensor (i.e., one that can

provide the kind and quality of data required by the mission), determination of target position, and provision of a means of fire control and adjustment. The benefits from applying man's memory, reasoning, and decisionmaking capacity in these processes is clear. In attempting to provide these capabilities, there are advantages to be gained in operating from an elevated platform close to the objective area, whatever specific capabilities might be required to accomplish the task. But this means employing an appropriate set of instrumentalities and operational concepts that satisfies the mission requirements within tolerable cost bounds. The developing image of the technologically advanced battlefield--large numbers of mobile, hard target elements that must be located precisely and struck accurately--combined with the environmental constraints of poor weather and rough terrain indicate that a low, slow, maneuverable platform is preferred. But the increasingly hostile environment over and beyond the FEBA caused by the growing surface-to-air defense system effectiveness makes the use of manned aircraft systems in this role extremely expensive in both personnel losses and dollar cost.⁴ One should not question whether such a situation will ever emerge to challenge the continuing viability of manned operations into enemy air space, it is only a matter of time and circumstance. Nor need all manned operations be called

⁴In response to this situation, the Army intends to augment its manned aerial observer with a mini-RPV. Their current Aquila program is aimed at developing the required operational capability for such a system. See Refs. 8 and 9.

into question. It is sufficient that some important mission areas be so challenged.

Concern over strong defenses is not a new phenomenon, as forces and equipment have been designed and operated all along to minimize their vulnerability to enemy weapons. But the severity of the threat is reaching such proportions that it is no longer feasible to rely on time-honored solutions aimed at permitting manned aircraft to penetrate enemy air space and to operate more or less as usual. But why must a manned aircraft be used for every type of Air Force mission? Aside from tradition, institutional self-preservation, and the natural human tendency to keep doing things the way one always has, there are no inherent characteristics in the missions described above that dictate the physical presence of a man in the target area. Certainly there are tasks required that only a man can do, or can do much better than an automatic device. But to accomplish them requires only that a man's intellect be able to perceive and react to elements present in the combat area. Technology has now made this possible in many circumstances through remotely piloted vehicles, adequate imaging sensors, and high-capacity, wide band data links that permit the man to function in an environment and location conducive to performance and safety.

Another approach, as mentioned above, is to reduce the air defense effectiveness to a tolerable level, so that manned aircraft

can operate over enemy territory with a reasonable probability of survival. In order for this to be possible, ground defenses would have to be destroyed, or at least suppressed, to reduce the number of threat elements operationally deployed and threatening the manned aircraft force. Defense suppression or "busting" is an important, difficult, and high-risk mission when performed by conventional manned strike forces. The use of remotely piloted vehicles to detect, locate, and designate defense targets for attack by standoff weapons would greatly enhance the defense suppression and destruction capability of manned aircraft.⁵

IV

As the enemy takes steps to degrade the weight and effectiveness of friendly air-delivered fire power, the need for such fire support intensifies as the enemy ground forces expand and modernize. Many studies have shown that NATO ground forces facing a Warsaw Pact assault in Central Europe would be fire power limited in their attempt to deal with the massive assault forces called for in Soviet operational doctrine. To alleviate this problem, one would like not only to increase the volume and rate of fire of friendly units, but also expand the killing zone over which the

⁵ Although not remotely piloted, the technical and operational feasibility of harassment drones designed to detect and home on defense radars are also worth exploring to assist in this task. See Ref. 5 for a brief description of an early USAF/ARPA experimental vehicle called Axillary.

enemy forces could be brought under fire. Artillery can augment fire power of forward defense elements, but it, too, is limited in volume, range, and ability to concentrate laterally along the battlefield. An airborne forward observer can expand the killing zone beyond the maximum firing range of the artillery, but is extremely vulnerable to modern air defense systems. But without his capability to find and designate battlefield targets such as armored fighting vehicles and artillery, the effectiveness of air-delivered fire power can be seriously degraded in a heavily defended environment. But as was argued earlier, these functions can be performed remotely by using a vehicle that, because of its low signature and small size, is more survivable than a manned aircraft and can operate close enough to the target to mitigate the degrading effects of weather, vegetation, and terrain. Moreover, compared to manned aircraft, the cost trends of providing these functions remotely may be favorable since loss rates should be lower than for manned aircraft, the unit cost of vehicles lost should be markedly less, and one can avoid the indeterminate (but highly undesirable) cost of lost aircrews.

The employment of remotely manned systems for combat area surveillance, target acquisition, and strike control against battlefield targets such as armor, artillery, and ground-to-air defenses could help offset the serious threat resulting from the incorporation of advanced technology by the enemy. For these applications,

the motivation for considering remotely manned systems derives from the ever-widening gap between the fire power of Warsaw Pact ground forces and the NATO defenders, coupled with the strengthening protective ground-to-air defensive shield covering the Pact armored assault forces. Continuing to hope to combat this situation with traditional manned ground attack aircraft and tactics will prove unconscionably expensive in terms of both personnel and monetary costs. Consequently, in this context, the introduction of a remotely manned system should be viewed as a complement and supplement to manned surveillance (i.e., forward air controller) and strike aircraft in a total force context, and as a hedge to cover those situations that will require the Air Force to provide vital supporting fires to ground forces, even though the use of conventional manned aircraft operations might suffer grievous losses.

To summarize, technological developments (such as remotely manned systems) are one promising approach to alleviating the risk to manned aircraft operations and, at the same time, to complementing and supplementing this capability. Thus, the developing threat and technological innovations on both sides are pointing toward solutions for military strike systems that must rely on data links to provide vital functions in their operations.

V

If the rationale that led up to this point is reasonable, what then is inhibiting the full-scale development of operational remotely manned systems for these tasks? One possibility is the fear that unmanned vehicles will turn out to be at least as vulnerable as manned aircraft to enemy weapons and countermeasures. These new devices do have their own vulnerabilities. Aside from the physical vulnerability (small size and low signatures help here), many mission functions, if they are to be performed by unmanned vehicles at all, require transmission of data in real (or near real) time over a data link from the vehicle to a remote control station. Thus, a new potential vulnerability (the link itself) is added to the tactical air-ground strike system. And it is one that is of a considerably different character than has been faced before by tactical strike force planners and operators.

Concern over the potential vulnerability of our weapons systems to electronic warfare has been publicly acknowledged. In a speech on 14 September 1976 to the 13th Annual Electronic Warfare Symposium of the Association of Old Crows, Malcolm R. Currie, then Director of Defense Research and Engineering, said that, "...photons, if you will--are every bit as important and central as bullets in fighting a war. Unfortunately for us, the Soviet Union understands this well and has devoted enormous amounts of equipment and manpower to electronic warfare." He then went on to say that, "For

this reason, we have issued DoD Directive 4600.3, which directs that electronic counter-countermeasures (ECCM) be specifically considered in the design of every system we develop for military use. ECCM must become an integral part of our planning--not a patchwork subsequent add-on."

Certainly, there is no question but that the data link offers the enemy an opportunity to degrade, or even negate the performance of the system of which the link is a part. But that is no justification to adopt (as many do) an unduly pessimistic assessment of data link vulnerability, particularly when made without benefit of rational analysis. That would seem to be a singularly unfortunate self-defeating attitude to take in view of the pressing need to adapt to the growing enemy ground-to-air defense capabilities against manned aircraft.

In large part, the foregoing state of affairs may be directly attributable to the traditional approach to the specification of jam resistance in electronic equipment. All hinges on the establishment of the enemy threat. This has usually been done by relying on approved intelligence estimates, or by invoking the "mirror image" doctrine, for example. The anti-jamming design requirements are then made sufficient to allow the needed function to be performed up to its specification in the face of the postulated threat. Moreover, this calculation is usually made out-of- context--on a one-on-one basis--and considers only the technological interactions

between the jammer and anti-jamming techniques. Hence, any specified level of jam resistance can always be overcome by postulating a more capable jammer threat as there is nothing in the process to inhibit or bound threat estimates. Common sense dictates otherwise--increasing performance, let alone unbounded capability, cannot come without cost. In following this approach, one can have only as much confidence in his jam-resistance specification (and, more importantly, in the operational utility of the combat system employing the data link) as he has in his estimate of enemy capabilities. In addition, there is no rational means of determining how much to pay for whatever level of jam resistance is settled upon.

One might be tempted to assert that the foregoing approach to ECCM is in consonance with Dr. Currie's admonition to make it "an integral part of our planning." In this case, is it not possible that planning, based on inadequate and incomplete analysis, will prove to be worse than none at all? It would have been better, perhaps, if rather less emphasis had been placed on the ECM/ECCM game itself and more on the system context within which the game is played. The crucial question is not whether one jammer can jam one data link, but whether a tactical strike force (including data links as vital elements) can be functionally cost-effective in the face of an enemy jamming system that he can introduce and support

as a technologically, operationally, and economically feasible component of his military establishment.

VI

At least a partial remedy to the difficulties associated with the analysis of data link vulnerability can be had by reverting to first principles. In this case, that means focusing on the principle of the objective. In this sense, the successful operation of the data link in the presence of enemy attempts to interfere is not a militarily-useful end product in and of itself. Presumably, however, a functioning data link is a requisite component of a system whose output is the desired military function. Thus, it would seem appropriate to measure the impact of the performance of the data link (i.e., the resultant of the interaction of the enemy jamming effort and the level of jam resistance built into the link) in terms of the extent to which the goal of the complete system or force has been met. In the case of a data link in a target surveillance and designation RPV, as described previously, the degradation due to enemy jamming (or, conversely, the remedial value of enhanced jam resistance) could be measured in terms of the change in the number of targets detected and destroyed, or the movement in the line of contact of the ground forces being supported, for example.

Clearly, the use of an operationally-oriented payoff function means that the analysis must be carried out within the context of a two-sided, air-ground campaign. But pointing out the rationality of employing a total systems context does not lead unfailingly to a single, appropriate, operationally-oriented measure. While those suggested above are appropriate, they are not unique. Moreover, there are likely to be other measures that vary inversely, indicating that enhancing one operational payoff may incur costs in another operational sense.⁶ For example, one offense option may increase target kills but suffer higher air vehicle attrition than another equal cost (monetary) option. One's preference must balance the desire to preserve one's force and the need to defeat the enemy. Aside from assessing the human and monetary costs, this calculation is somehow related to one's estimate of the expected duration of the conflict, the likelihood and timing of replacements, the criticality of the enemy targets, the urgency of their destruction, and the degree to which the requisite damage can be inflicted upon them, among other things. As in most systems analysis problems, the choice of payoff criterion is one of, if not, the most critical and difficult tasks facing the analyst.⁷

⁶Monetary costs, of course, must be included also and are discussed below.

⁷A discussion of the relationships among objectives, criteria, and costs, together with the difficulties of their definition and measurement for complex defense system decision problems, is given in Ref. 10.

To have any hope of avoiding the open-ended escalation of the traditional kW vs. db argument, the monetary costs incurred by both sides must be included, along with the purported benefits. That these costs should include all elements of the life-cycle expenditures should be self-evident. Moreover, total system life-cycle costs are an essential measure when examining alternative ways of allocating resources--and there are alternatives to jamming and jam resistance open to both defense and offense in this case. Consequently, the preferred level of the electronic countermeasures game cannot be sought independently of an assessment of its desirability vis-a-vis alternative techniques that would permit either side to attain its combat objectives.

Consider an obvious option open to the defense when confronted with the introduction of an effective target detection and attack system in which a data link is a vital element. The defense planner should ask himself whether he can obtain a greater payoff for his investment from introducing a new electronic jamming system, or from simply adding an equal investment in more and/or better weapons to his already-existing active defense system. In principle, then, this point of view can be the basis for a rational criterion for deciding how much jam resistance it makes sense to demand in a data link and at what cost. That is, the jam-resistance performance requirement could be set at a level that would cost the defense just as much to try to jam the data link as it would to try

to shoot down the air vehicles. More specifically, for a given degree of protection (i.e., survival) afforded the targets under attack, an attack system with data links of the specified level of jam resistance would force the defense to a jamming system of a cost equal to that of an active defense system that would provide the same degree of target survival by shooting at the attacking air vehicles. This is the key concept: provide only enough jam resistance to make the enemy's jamming system sufficiently complex and costly that other alternative uses of his defense budget appear more attractive to him. In essence, we seek to configure our entire offense system in a way that presents no soft spots for the enemy to exploit at relatively low cost and high effectiveness. This permits the enemy defense planner no obviously preferred allocation of his budget and, hopefully, puts the offense in a position that would not be seriously degraded, regardless of which of its available options the defense might choose.

VII

To this point, the discussion has focused on motives for concern over the vulnerability of RPV data links and has suggested a way to approach the analysis of that problem. Now we must examine the components of the ECM/ECCM game and seek to identify and elucidate their interactions. We begin by recognizing that there will be specific forces and equipments in being at the time that a new

element relying on a data link is introduced by the offense. This means that a marginal analysis approach must be taken in considering the impact of the introduction into operational use of a new technological product.

If, as an example, we consider the use of a target acquisition and designation RPV in the near future, it is reasonable to postulate that the enemy will not have an appropriate jamming capability deployed at the time that the RPV first becomes operational. In attempting to plan for subsequent events, we must examine a series of incremental and sequential moves and countermoves by each side to seek insight regarding:

1. The kinds of options available to each side.
2. The circumstances under which the defense might be motivated to add a jamming system to his existing active defenses and those where the offense is motivated to respond by adding additional jam resistance to the data links (as opposed to simply buying more target acquisition RPVs and strike aircraft).
3. The feasibility of establishing the data link jam-resistance performance requirements and the associated upper bounds on their costs as a function of the rational defense options.
4. Finally, the penalties associated with each possible

offense/defense option in the event the other side spends his incremental budget other than anticipated.

If the enemy chooses to increase his defense budget in an attempt to counter the newly-acquired RPV capability, he can, of course, spend this additional budget increment entirely on more or better active defense, on developing and introducing a jamming system, or on a combination of the two. For a given incremental defense budget, it is possible to establish the minimum jammer system effectiveness required at a given jammer cost necessary to provide the same level of target survival as would result from an equal investment in additional active defenses. With the incremental defense budget allocated to either a jamming system of the minimum required capability or to additional active defenses, the enemy target survival will be increased by the same amount over that obtaining for the original defense budget level. With any lesser capability in jammer technology, there would be no incentive for the defense to opt to employ jammers.

VIII

The countermove to all of this by the offense is to increase his budget some amount with the intention of returning to the target survival level of the original offense/defense budgets and force configurations.⁸ The question is, what are the available

⁸The criterion by which to establish the offense budget level increment is, of course, a subjective judgement involving the

options for the offense and how much budget increase does each require? The answers to these questions depend upon which of his options the defense has chosen to exercise. Let us suppose, for the moment, that the offense is accurately informed as to the chosen defense option. In that event, the appropriate offense response to an incremental defense budget devoted entirely to additional active defense would be to invest some additional amount in a suitable mix of target acquisition RPVs and strike aircraft in a quantity sufficient to decrease the enemy target survival to the desired original level. Alternatively, if the defense chose to purchase a jamming system, the offense choice is somewhat more involved, as there are two ways to counter the jamming threat--add ECCM to the data links, or ignore the jamming and proliferate the target acquisition vehicles to the extent necessary to overwhelm the jamming system.⁹

By examining the two offense options that rely simply on increased force size to counter the incremental enemy defense investment, the offense can determine the additional cost required in

degree of satisfaction with the original state of target survival and estimates of which side (if either) stands to gain from a budget race, for example. The illustrative example of simply seeking to return to the status quo ante is but one intuitively attractive choice.

⁹The latter offense tactic of overwhelming the jamming system with numbers would, in general, not result in an offense force composition or cost identical to the first-mentioned offense option. This is because one option sizes the offense force mix to operate against an all active defense threat, while the other is designed against a mixed active and jamming defense.

each case. These values can then be viewed as cost bounds on the permissible investment in the third offense option--added jam resistance in the data link. For this option to be competitive with either of the others, the target survival must be reduced to the original level solely by providing ECCM (jam resistance) in the data link. This means that the added jam resistance must be able to completely defeat the enemy jamming effort at a cost within the indicated bounds.

If the offense planner believes that the defense has the technological capability to produce jammers of at least the minimum performance required to be competitive with active defenses and, moreover, that he will opt to enhance his existing defenses by adding such jammers, then it is possible to derive performance and cost guidelines that must be met by any added data link jam-resistance equipment. There are many combinations of necessary jam resistance and associated cost available to the offense that will return the level of target survival to its original value. This range of combinations occurs because it is possible for the offense to employ mixed options that devote varying amounts of the budget increment to incorporating jam-resistance techniques and to buying additional vehicles. The result is that a tradeoff boundary exists with varying values of the minimum necessary jam-resistance performance and the allowable cost, depending upon the proportion of the offense budget increment devoted to improving the data link jam resistance.

IX

The previous discussion of offense options has dealt, for simplicity, with the situations that result from perfect knowledge on the part of the offense with regard to how the defense has chosen to allocate his budget increment. However, it is not likely that the offense would have perfect a priori knowledge of the defense decision and would have to structure his planning under some uncertainty.¹⁰ Therefore, it seems prudent to examine the consequences associated with each offense option in the event that the defense actually chooses an option other than that anticipated. Conceivably, minimizing any such penalties could serve as a supplementary selection criterion for the offense in choosing among otherwise equally desirable options.

The set of offense and defense options and their rational combinations are enumerated in Fig. 1. As identified by A through F, there are only six combinations of circumstances (i.e., offense estimate of the selected defense option, the actual defense choice, and the actual offense option) that are logically consistent.¹¹

¹⁰ This would be particularly the case if the offense were attempting to anticipate rational defense moves so that appropriate design and performance characteristics could be incorporated in advance. That is, although we have structured our discussion of the ECM/ECCM game as if move and countermove followed one another sequentially in time, in reality, it is more likely that offense and defense would be planning and implementing their options more or less in parallel.

¹¹ For example, it would make no sense for the offense to devote its budget increment to adding jam resistance to the data link

Consider, first, the instance in which the offense believes that the defense has chosen to invest in additional active defenses and, therefore, the offense devotes his incremental budget only to increasing the size of his target acquisition and strike vehicle force. And if the defense had, in fact, opted for increased active defense, each side would have spent its incremental budget in the appropriate way to match the other's move (i.e., Case A). As was discussed earlier, the incremental offense budget required in this case to reduce the target survival level to its original value is one criterion that can be used to derive performance and cost guidelines for adding jam resistance to the data link in the event the defense is believed to have invested in a jamming system (as will be discussed later for Cases D and F).

On the other hand, suppose the defense actually had chosen to add a jamming system, although the offense believed to the contrary (i.e., Case B). Now, the offense force mix is mal-distributed, since it has been configured on the basis of an active defense strength greater than it will actually encounter and because no attempt has been made to counter-balance the effect of jamming. Consequently, the target survival level will be higher (i.e., more favorable to the defense) than in Case A. How much higher will

if it believed the defense had invested in additional active defenses. It should be noted also that for either offense Option 1 or 2, the data links in the additional acquisition vehicles remain unaltered, i.e., no jam-resistant features are added.

depend upon the specific values of the performance, cost, and scenario parameters of the situation being analyzed. The important point is that some penalty to the offense will result and knowledge of it should be included in his planning process.

When the offense believes that the defense has chosen to add a jamming system to his active defenses, the appropriate offense response is either to invest in additional jam resistance for the data link, or to leave the link unaltered and add vehicles in a proportion optimized against the mixed active and jamming defense system it expects to encounter. These two offense alternatives give rise to two sets of possible outcomes (Cases D and F, and C and E, respectively), depending upon which option the defense has actually implemented.

Were the offense to choose offense Option 2, the resulting situations (Cases C and E) would be similar to Cases A and B, respectively. That is, for the on-design¹² event (Case C), the incremental cost of the added acquisition and strike vehicles necessary to meet the original target survival level can provide another guide to the needed jam resistance and its allowable cost. Here, too, if the defense is not configured as anticipated (Case E), the resultant target survival will favor the defense because of the mal-proportioned offense vehicle mix.

¹²We will denote by "on-design" any case in which the defense actually chooses the option that the offense estimates it will, and by "off-design" any case in which the actual defense option and the offense estimate diverge.

If the offense is able to meet the performance and cost requirements dictated by the guidelines derived from Cases A and C and opts to put the entire incremental budget into jam resistance, by definition, then the target survival level will be returned to its original value. However, if the defense actually had chosen to increase the active defenses, then the target survival would be unaffected by the added offense expenditure (i.e., the offense would gain nothing for his efforts), as none of it would have been used to add to the original offense force mix to counteract the increase in active defense strength. An offense option allocating part of the budget increment to jam resistance measures and part to increasing the vehicle forces would obviously lie somewhere between the two extremes.

X

To this point, we have discussed only the consequences of facing a defense jamming system with the minimum capability required to make that option perform as well as if the defense had made an equal investment in additional active defenses. Would a substantially different situation result if the defense jammer capability were greater--either better technical performance, lower unit cost, or both--than the minimum? To answer that question, we need a rationale for establishing how large an increase in the offense budget is needed to completely negate the enemy

jamming capability. In deriving the minimum enemy jamming requirement, we were able to establish the offense budget increment by equating it to that needed to completely offset a defense increase devoted entirely to additional active defenses. In this case, an analogous approach is to determine the offense budget increment necessary to overwhelm the jamming system with numbers rather than by countering it through electronic means. Clearly, if the defense jammer capability is greater, the incremental offense budget needed to overcome it is larger than if matched against a jammer system with only the minimum required capability. Consequently, the jam-resistance performance and cost tradeoff boundary is everywhere greater when the defense employs jammers whose capability exceed the minimum required to match the effectiveness of an equal-cost active defense increment. Since both the necessary jam resistance and allowable cost values are greater, it is difficult to determine, in general, whether an enemy jammer capability greater than the minimum required would pose a more severe problem. State-of-the-art performance and cost estimates for both sides would be needed to answer that question.

XI

In summary, changes are being introduced into the classical tactical battlefield environment as both sides incorporate weapons of advanced technology into operational use. One important

development is the increasingly hostile environment to be expected over enemy ground forces stemming from highly effective and numerous surface-to-air defenses. Consequently, the continuing use of manned aircraft to accomplish target development, acquisition, identification, and designation for accurate, effective weapon delivery will become extremely expensive in both personnel losses and dollar cost. Remotely piloted systems are aimed at mitigating this problem.

A data link is a mission-essential element of a remotely piloted vehicle system. This introduces the possibility that the vulnerability of those links could prove to be an attractive opportunity for the enemy to exploit to combat RPVs. Consequently, there is a need for rational analysis on this point to avoid the unfortunate consequences of either undue optimism or pessimism regarding the outcome of the ECM/ECCM game. Such an analysis needs to put the ECM/ECCM game in its proper context as only one part of a complete combat system, to utilize a performance measure associated with the military function of the system as a whole (not just the operation of the data link), and to consider alternative solutions with their associated life-cycle costs (not just procurement costs). Taking a systematic approach to the problem should make it possible to assess the options available to each side, the circumstances favoring one or another option, the penalties incurred in the event the other side behaves other than anticipated,

and to derive guidelines for the necessary data link jam resistance and its allowable cost.

It would appear that there can be no general, definitive answer to the question of whether the defense would prefer to jam a data link rather than augment existing active defenses, since there will always be uncertainties regarding one's apparent knowledge of enemy technological/cost capabilities and motives. The particular context and the specific technological and cost-estimates thought to be appropriate will dictate the specific answer, as is usually the case in complex combat analyses. But given that an appropriate systematic analysis indicates a motivation on the part of the defense to employ jamming, then it should also be possible to provide offense planners with rationally-derived, jam-resistance performance and cost guidelines for data links.

Defense Options

1. Add more active defenses
2. Add a jamming system

Offense Options

1. Add more target acquisition and strike vehicles
(vehicle mix optimized against Defense Option 1)
2. Add more target acquisition and strike vehicles
(vehicle mix optimized against Defense Option 2)
3. Add jam resistance to acquisition vehicle data link
(vehicle mix optimized against Defense Option 2,
accounting for increased acquisition vehicle cost)

Rational Combinations

	<u>Offense Estimate of Defense</u>	<u>Offense Choice</u>	<u>Actual Defense</u>
A.	Defense Option 1	Offense Option 1	Defense Option 1
B.	Defense Option 1	Offense Option 1	Defense Option 2
C.	Defense Option 2	Offense Option 2	Defense Option 2
D.	Defense Option 2	Offense Option 3	Defense Option 2
E.	Defense Option 2	Offense Option 2	Defense Option 1
F.	Defense Option 2	Offense Option 3	Defense Option 1

Fig. 1--Defense and Offense Options with Their Rational Combinations

REFERENCES

1. Shore, David, "RPVs in Future Combat," *National Defense*, Nov.-Dec. 1976, pp. 205-208.
2. Ulsamer, Edgar E., "Remotely Piloted Aircraft - Weapon Systems of the Future?", *Air Force and Space Digest*, Oct. 1970, pp. 40-44.
3. Miller, Barry, "RPVs Provide U.S. New Weapon Options," *Aviation Week and Space Technology*, January 22, 1973, pp. 38-43.
4. Brownlow, Cecil, "Operational Decisions Pace Advance," *Aviation Week and Space Technology*, January 22, 1973, pp. 50-56.
5. Miller, Barry, "Mini-RPV Research Programs Expanded," *Aviation Week and Space Technology*, March 4, 1974, pp. 17-18.
6. Klass, Philip J., "Mini-RPV Program Spawns Wide Range of Vehicles," *Aviation Week and Space Technology*, July 14, 1975, pp. 49-50.
7. U.S. Congress, Report of Senator Sam Munn and Senator Dewey F. Bartlett to the Committee on Armed Services, United States Senate, *NATO and the New Soviet Threat*, Committee Print, U.S. Government Printing Office, Washington, D.C., January 24, 1977.
8. Klass, Philip J., "Army Begins Priority Mini-RPV Program," *Aviation Week and Space Technology*, July 1, 1974, pp. 20-21.
9. Walsh, Bill, "Aquila RPV Update," *EE&I Countermeasures*, May 1976, pp. 22-23.
10. Attaway, L. D., "Criteria and the Measurement of Effectiveness," *Systems Analysis and Policy Planning: Applications in Defense*, edited by E. S. Quade and W. I. Boucher, New York: American Elsevier Publishing Company, Inc., 1968.